AO 91 (Rev. 11/11) Criminal Complaint (approved by AUSA Sarah Wolfe)

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

United States of America
v.
Terrell Ashby, a/k/a "Jason Brandon"

Case No. 20-mj-2182

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 22, 2020 in the county of Delaware in the Eastern District of Pennsylvania, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2261A(2)	On or about August 22, 2020, in the Eastern District of Pennsylvania, the defendant, Terrell Ashby (a/k/a "Jason Brandon"), with the intent to injure, harass, and intimidate another person, used interactive computer services and electronic communication services of interstate commerce, including Internet-based social media platforms and electronic messaging applications, to engage in a course of conduct that caused substantial emotional distress to that person, in violation of Title 18, United States Code, Section 2261A(2).

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT.

☑ Continued on the attached sheet.

s/ Jeffrey Hunter
Complainant's signature

Jeffrey Hunter, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/17/2020 at 4:09 p.m.

s/ Hon. Richard A. Lloret
Judge's signature

City and state: Philadelphia, PA

The Hon. Richard A. Lloret, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AFFIDAVIT

I, Jeffrey Hunter, being first duly sworn, hereby depose and state as follows:

A. Introduction and Agent Background

1. I make this affidavit in support of a Criminal Complaint and Arrest Warrant against TERRELL ASHBY. As set forth below, there is probable cause to believe that TERRELL ASHBY, with the intent to injure, harass, and intimidate another person, used interactive computer services and electronic communication services of interstate commerce, including Internet-based social media platforms and electronic messaging applications, to engage in a course of conduct that caused substantial emotional distress to that person, in violation of Title 18, United States Code, Section 2261A(2).

2. I am currently a Special Agent with the United States Department of Justice, Federal Bureau of Investigation (FBI) and have been since November of 2006. Prior to becoming a Special Agent, I was employed as a Detective with the Chicago Police Department, where I worked as an Officer and Detective since January of 2000. Over the course of my career I have investigated homicides, robberies, kidnappings, burglaries, firearms violations, sexual assaults, narcotics violations, frauds, and numerous other crimes. I am currently assigned to the FBI Philadelphia Division's Cyber Crime Squad, whose primary mission is to investigate crimes involving computers and the internet. Based upon my training and experience, I am familiar with the means by which individuals use computer and information networks such as the Internet to commit various criminal offenses, and I have participated in the execution of searches and

seizures pursuant to warrants authorizing the seizure of evidence related to computer crimes. I have also executed numerous arrest warrants based on federal criminal violations.

3. This affidavit is based on my personal knowledge and information obtained from documents, witnesses, and other law enforcement officials. The information contained in this affidavit is submitted for the limited purpose of establishing probable cause in support of a criminal complaint and arrest warrant against TERRELL ASHBY. As such, this affidavit does not include all of the information that I have acquired while participating in this investigation.

B. Statement of Probable Cause

4. At all times relevant to this Complaint, Provider A was a social-media platform and Provider B was an electronic messaging application. Both Providers A and B provided users the ability to engage in private conversations, with chat and/or video, and to publish content viewable by other users. Provider C is a peer-to-peer payment processing application.

5. On or about August 22, 2020, a 20 year-old female ("Victim 1"), who was residing in the Eastern District of Pennsylvania, interacted online with an individual known to her as "Jason Brandon" and subsequently identified by law enforcement as TERRELL ASHBY ("ASHBY"). Victim 1 originally received a message from ASHBY (who was using account "jbrand0n.1993" on Provider A's platform), offering Victim 1 a large sum of money and enticing her to communicate with him on Provider B's platform. Victim 1 agreed and subsequently engaged in a nude video chat with ASHBY (who was using account "jasonbrandon199" on Provider B's platform).

6. Unbeknownst to Victim 1, ASHBY recorded portions of their video chat, and subsequently sent Victim 1 multiple messages via Provider B demanding $40 in exchange for deleting a nude photo he had captured of her. Specifically, ASHBY (using account

"jasonbrandon199") wrote, in part, "When you send the $40 I will delete your nudes offline" and "Just send the $40 and you're good lol[.] We aren't good until you send the $40[,] simply send the $40 and I'll delete it[.]" Victim 1 then paid the $40 by transferring money via Provider C's online payment platform to an account with username "slispopas4" as provided by ASHBY.

7. However, ASHBY then sent Victim 1 multiple messages via Provider B demanding all of the money in Victim 1's bank account. In these messages, ASHBY (using account "jasonbrandon199") threatened to disseminate the nude photos of Victim 1 to her college and other social media friends and followers if she did not pay him more money. For example, ASHBY wrote, in part:

> Your expose page is being created right now and I'm also going to tag your college[.] I'll end you[.] I'm not someone you want to [expletive] with[,] go tell your father that
> …
> Just [sent] your nudes to [name redacted]
> Already exposed you whore
> Your life is over
> You're dumb if you thought this was over its not over until my $134 is sent
> I'll make sure our whole school sees your nudes

8. As a result of ASHBY's conduct, Victim 1 became distraught and ingested a number of prescription pills in an attempt to calm her emotional distress. She was rushed to an emergency room in an ambulance and ultimately recovered.

9. While Victim 1 was hospitalized, on August 22, 2020, ASHBY began advertising the nude photos of Victim 1 using various accounts on Provider A and Provider B, including the following:

a. On Provider A's platform, ASHBY posted a photo of Victim 1 using an account named "[name redacted]sextape" with the following caption:

> Everyone [message] me to see [Victim 1] nudes … she [video chatted] me naked I have the full [video chat] call saved [message] me to see everyone.

b. On Provider B's platform, ASHBY added a nude photo of Victim 1 to the profile of his "jasonbrandon199" account with the following caption: "[e]veryone slide up to see @[Victim 1]."

c. On Provider B's platform, ASHBY created a new account with username "[Victim 1]_nud20" and vanity name "[Victim 1].NUDES.ON.[Provider A]" and sent invitations to Victim 1's contacts, thereby advertising that Victim 1's nude photos could be seen on Provider A's platform.

10. Subsequently, on September 1, 2020, ASHBY continued to advertise Victim 1's nude photos by creating another new account on Provider B's platform, with username "[Victim 1]2020" and vanity name "[Victim 1]NUDES.EXPOSED."

11. Pursuant to subscriber records from Provider A and Provider B,

a. "jbrand0n.1993" (the account ASHBY used to solicit Victim 1) was registered on August 2, 2020 at 9:51 a.m. (EDT) from Internet Protocol (IP) address 2600:1003:b44d:8f2f:85da:b55d:acb3:9eb3;

b. "jasonbrandon199" (the account ASHBY used to capture the nude photos and subsequently extort Victim 1) was registered on May 27, 2020 at 9:59 a.m. (EDT) from IP address 2600:1003:b46c:3f60:f103:6dca:4a7c:817;

c. "[name redacted]sextape" (an account ASHBY used to advertise nude photos of Victim 1 on Provider A's platform) was registered on August 21, 2020 at 6:42 p.m. (EDT) from IP address 2600:1003:b466:76f:11eb:ce0b:9cdc:5052;

d. "[Victim 1]_nud20" (an account ASHBY used to advertise nude photos of Victim 1 on Provider B's platform) was registered on August 22, 2020 at 3:28 a.m. (EDT) from IP address 2600:1003:b45f:2f68:c108:cffa:8c87:c63b; and

e. "[Victim 1]2020" (another account ASHBY used to advertise nude photos of Victim 1 on Provider B's platform) was registered on September 1, 2020 at 12:01 a.m. (EDT) from IP address 2600:1003:b453:f003:7450:fcd:1cfe:382d.

12. All five of the above referenced IP addresses belong to Verizon Wireless. According to Verizon records, on the relevant dates, these IP addresses were all assigned to the same subscriber: a family member of ASHBY, with a residential address in Williamsburg, Virginia (the "Residential Address"). Verizon records further revealed that this subscriber account was associated with telephone number 757-903-8324, which was assigned to the following device: an Apple iPhone 7 Plus, with a corresponding International Mobile Equipment Identity (IMEI) number of 355834084459611 (the "Apple iPhone 7").

13. According to records from Apple, the Apple iPhone 7 is registered to ASHBY with two listed addresses, one of which is the Residential Address. Additional records from Apple revealed that on or about August 22, 2020, at approximately 7:05 a.m. (EDT), the Apple iPhone 7 received iTunes updates while assigned IP address 174.226.20.118. According to records from Provider B, on the same day approximately three hours later (*i.e.*, at 10:09 a.m. (EDT)), the same IP address was used to log into "jasonbrandon199" (the account used to capture the nude photos and extort Victim 1). Other iTunes updates sent to the Apple iPhone 7 revealed additional IP address crossover with the accounts ASHBY used to advertise Victim 1's nude photos on Provider B's platform.

14. Furthermore, records from Provider C confirmed that on August 22, 2020, at 2:49 a.m. (EDT), account "slispopas4" received a $40 transfer from Victim 1. The records also show that, less than 20 minutes later, at approximately 3:06 a.m. (EDT), $40 was transferred from the

"slispopas4" account to a Visa debit card ending in 7885 issued by Langley Federal Credit Union based in Newport News, Virginia.

15. Records from Langley Federal Credit Union identified the customer associated with Visa debit card ending in 7885 as ASHBY, with the Residential Address.

16. According to the Virginia Department of Motor Vehicle Driver's License records, ASHBY is a 22 year-old male with a current driver's license listing the Residential Address.

17. Additional records checks revealed that ASHBY has had several law enforcement contacts involving threatening, harassing, and violent behavior. One of these incidents (documented in a James City County Police report) occurred in August of 2017 when ASHBY was 19 years of age. The police report documents allegations made by a juvenile female victim that ASHBY was harassing her by sending her threatening text messages (including death threats) and calling her from several phone numbers. In another incident, in 2018, ASHBY was arrested and charged with domestic assault for allegedly pushing his mother during an argument. All of the police reports list ASHBY's address as the Residential Address, and also identify ASHBY's parents who reside at the Residential Address as well.

18. On October 22, 2020, FBI surveillance observed ASHBY in the front yard of the Residential Address near the front door.

19. On November 1, 2020, Victim 1 received another extortionate message from ASHBY, who was using a new account on Provider A's platform with the name "jbrandon1993_3". The extortionate message read as follows:

> Remember those pics you sent me and I posted and that [video chat] i screenrecorded? I'm not stopping until you send what you owe[.] I [messaged] 50 people you follow the pics you sent me

20. According to Provider A records, the "jbrandon1993_3" account was registered on October 29, 2020 from IP address 2600:8805:3a00:e1a:9d15:f3fc:d182:6266. This IP belongs to Cox Communications, a home digital cable and internet service provider, and is associated with the Williamsburg, Virginia geographic area.

s/ Jeffrey Hunter
Jeffrey Hunter, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me on December 17, 2020 at 4:09 p.m.

s/ Honorable Richard A. Lloret
THE HONORABLE RICHARD A. LLORET
United States Magistrate Judge
Eastern District of Pennsylvania